How To Use

Mobile Forensics

Reader & Viewer

Aung Zaw Myo

www.forensicsmyanmar.com

Forensics Reader Or Viewer

Forensics Reader တွေကို ဘယ်အချိန်မှာ အသုံးပြုလဲဆိုရင် Organization တစ်ခုကနေ တစ်ခုကိုလွှဲပြီး Analysis လုပ်ထားတဲ့ Case ကို မှန်လားမမှန်ဘူးလား ဘာတွေလိုအပ်နေလဲ ဘာတွေထပ်ပြီး Analysis လုပ်ဖို့လိုမလဲဆိုတာ ကိုကြည့်ဖို့ အတွက် အသုံးပြုပါတယ်။

ဘာလို့ Reader ကိုသုံးတာလဲဆိုရင် Organization A က UFED သုံးတယ်။ အကြောင်းတစ်စုံတစ်ရာရှိလို့ Organization B ကနေ Check လုပ်ရမယ်ဆိုရင် Organization B မှာ UFED မရှိရင် အခက်ခဲရှိပါတယ်။ ဒါကြောင့် Readers ကို အသုံးပြုပြီး Organization A က Analysis လုပ်ထားတဲ့ Case File ကိုဖွင့်ပြီး Analysis လုပ်လို့ရပါတယ်။ Organization တစ်ခုတင်မဟုတ်ပါဘူး။ Investigator တစ်ယောက်နဲ့ တစ်ယောက် Cross Check လုပ်တဲ့နေရာ။ တရားရုံးလိုနေရာ မျိုးတွေ မှာပါ အသုံးပြုပါတယ်။

ပြည်ပ တရားရုံးတွေမှာဆိုရင်လဲ Investigator Or Examiner ကနေ Analysis ထားတဲ့ Case File ကို သံသယရှိရင် ဒါမှမဟုတ် အကြောင်းတစ်စုံတစ်ခုရှိလို့ ဖွင့်ပြဖို့ လိုအပ်တယ်ဆိုရင် Reader ကိုအသုံးပြုပါတယ်။ Mobile Forensics Products တွေက အပေါ်က ကိစ္စတွေလိုမျိုးမှာ Reader ကိုအများဆုံးအသုံးပြုပါတယ်။ အချို့ Products တွေကတော့ Viewer လို့လဲခေါ်ပါတယ်။

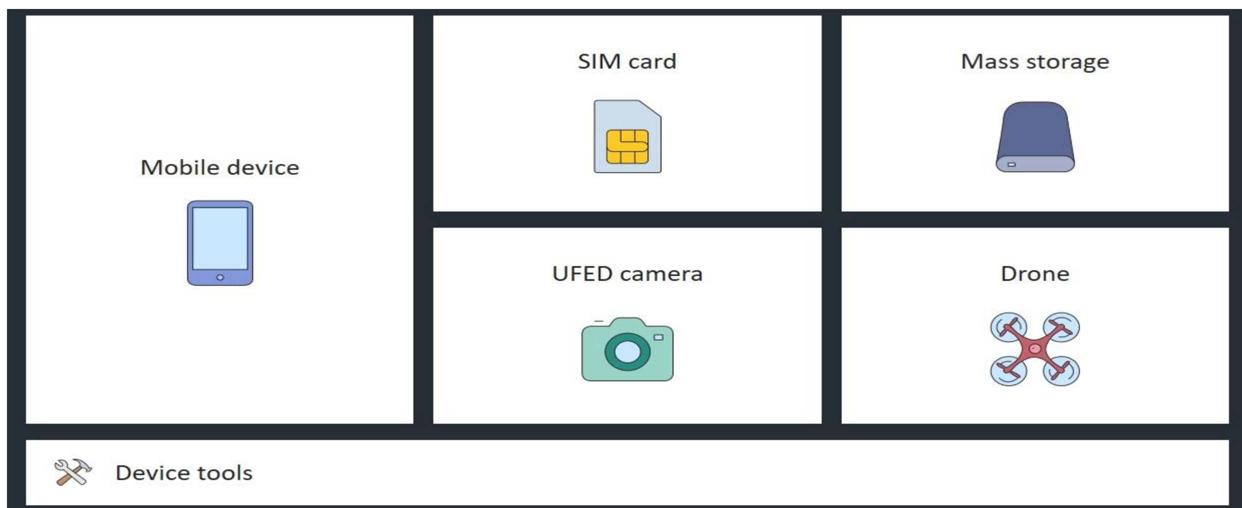
ကမ္ဘာမှာ အသုံးအများဆုံး နာမည်ကြီးတဲ့ Mobile Forensics Products တွေမှာလဲ Reader, Viewer အသီးသီးရှိပါတယ်။ သယ်ဆောင်အသုံး ပြုလို့လွယ် ကူအောင် Forensics Reader, Viewer တွေရဲ့ Size က 100 MB လောက် သာရှိပါတယ်။ Install ပြုလုပ်ဖို့ မလိုအပ်ပဲ Portable အနေနဲ့ အသုံးပြုနိုင်ပါတယ်။

Cellebrite UFED ဆိုရင် UFED Reader, MSAB (XRY) ဆိုရင် XAMN Viewer, Oxygen ဆိုရင် Oxygen Forensics Viewer

Forensics Reader , Viewer တွေအတွက် ပိုက်ဆံပေးစရာမလိုအပ်ပါဘူး။ အသုံးပြုတဲ့ Products အလိုက် အလွယ်တစ်ကူ Download ယူလို့ရပါတယ်။

UFED READER

Cellebrite က Mobile Forensics အတွက် UFED4 PC နဲ့ UFED Physical Aanalyzer ဆိုပြီး 2 မျိုးရှိပါတယ်။ UEFD4 PC က Forensics Workstation Or Computer မှာ Install လုပ်ပြီးအသုံးပြုပါတယ်။ UFED4 PC လိုပဲနောက်တစ်မျိုးမက Portable အနေနဲ့အသုံးပြုတာဖြစ်ပါတယ်။ UFED Touch လို့ခေါ်ပါတယ်။



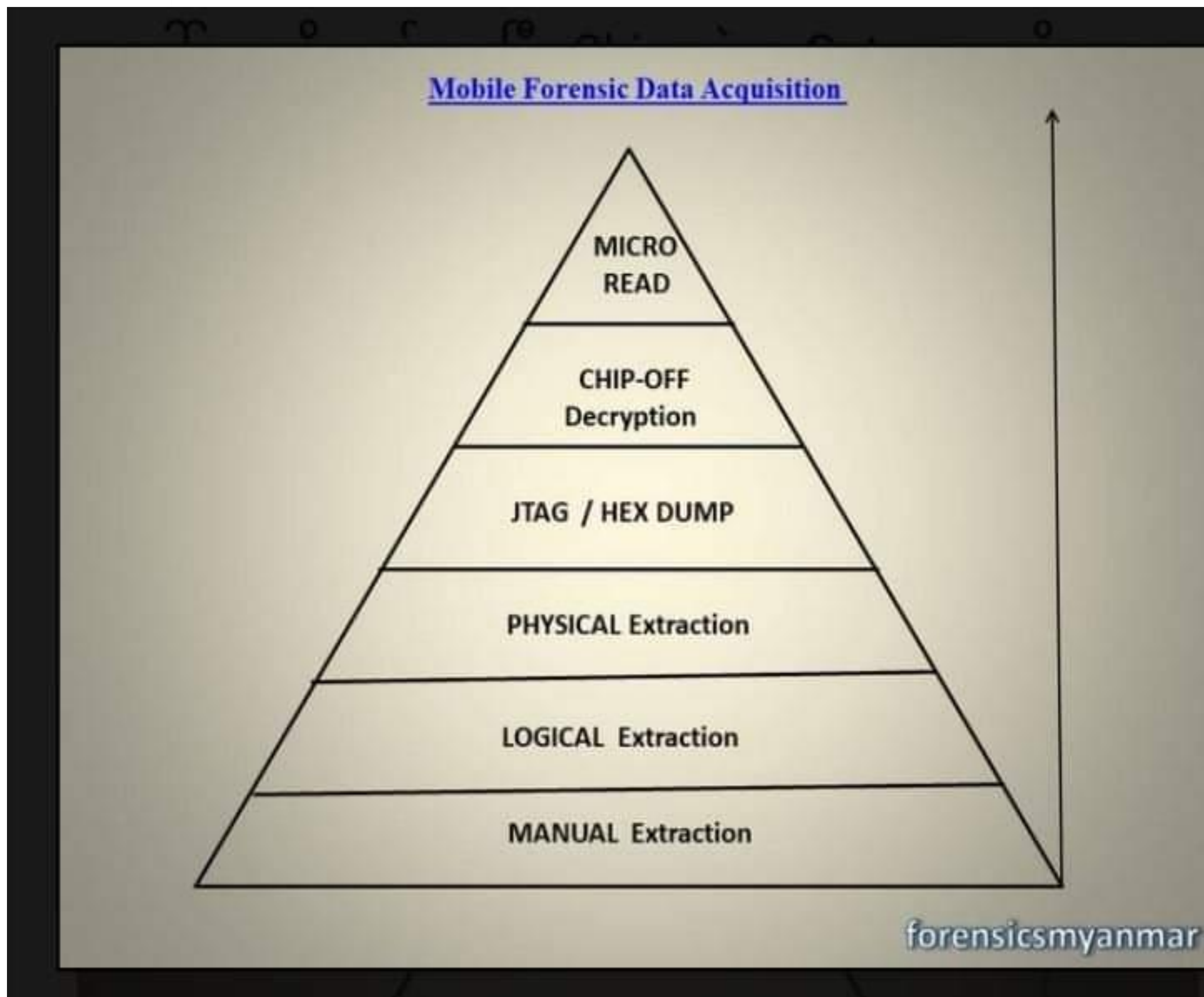
UFED4 PC Application



UFED Touch

World Wide မှာ အများဆုံး အသုံးပြုတဲ့ Mobile Forensics Product တွေထဲကမှ Forensics Reader , Viewer အကြောင်းကို UFED Reader နဲ့ နမူနာထားပြီး ရေးသားသွားပါမယ်။ ရေးတဲ့အချိန် ကျန်တဲ့ Product တွေရဲ့ Case File အဆင်သင့်မရှိလို့ပါ။ UFED Reader ကိုနားလည်အသုံးပြုတတ်ရင် ကျန်တာတွေက ပုံစံရော သဘောတရားရော အတူတူပါပဲ။

UFED4 PC နဲ့ ဖုန်းကိုစစ်ဆေးလိုက်တဲ့အခါမှာ ရလာတဲ့ Analysis Result ကို .UFED Extension အနေနဲ့ထွက်လာပါတယ်။ .UFED Extension UFED Physical Analyzer နဲ့ဖွင့်ပြီး Analysis လုပ်ဖို့အတွက်ဖြစ်ပါတယ်။ .UFED Extension File က UFED နဲ့သာဖွင့်လို့ရအောင်ပြုလုပ်ထားတာဖြစ်ပါတယ်။ နောက်ပိုင်းမှာတော့ Mobile Forensics Product အချို့မှာပါဖွင့်လို့ရလာပါတယ်။ Analysis ပြုလုပ်ဖို့အတွက် ရလာတဲ့ File Size ကတော့ Phone Storage နဲ့ Examiner ကနေ Data Extraction ပြုလုပ်တဲ့အပေါ်မူတည်ပြီး Size အမျိုးမျိုးရှိနိုင်ပါတယ်။ Mobile Data Extraction (Acquisition) နဲ့ပတ်သတ်ပြီး အနည်းငယ်သိထားရမဲ့အပိုင်းတွေရှိပါတယ်။ Mobile Phones တစ်လုံးကို Analysis လုပ်ဖို့အတွက် ပထမဆုံး သိထားရမဲ့ Acquisition နည်းလမ်းတွေကတော့ ---



Manual Extraction

သံသယရှိသူထံကနေ Mobile Device ကို စတင်သိမ်းဆည်းတဲ့အခါမှာ Mobile Device ကိုကြည့်ပြီး အသုံးပြုနေတဲ့ App / သိမ်းဆည်းနေတုန်းမှာ အချက်အလက်တွေကို ဖျက်နေတာတွေရှိနိုင်လား အသုံးပြုနေတဲ့ Telecom / Wireless AP စတာတွေနဲ့ ဖုန်းမှာ အသုံးပြုထားတာတွေကို ဓာတ်ပုံ ဗီဒီယို မှတ်တမ်းတင်ခြင်း၊ document ရေးသွင်းခြင်းတို့ဖြစ်ပါတယ်။ Manual Extraction လုပ်တဲ့အချိန် Manual Extraction လုပ်တဲ့ ဖုန်းထဲမှာ Screenshoot ရိုက်တာမပြုလုပ်သင့်ပါဘူး။

Logical Extraction

Mobile Device ထဲမှာ လက်တလောရှိနေတဲ့ Memory Storage ထဲကနေ System data / user data စတဲ့အချက်လက်တွေကို ကူးယူခြင်းဖြစ်ပါတယ်။ ဖုန်းကို Back

Up ယူတာနဲ့ဆင်တူပါတယ်။ အချို့သော ဖုန်း OS အမျိုးအစား Model အလိုက် Logical Extraction ကနေ Recovery ပြန်ရနိုင်ပါတယ်။ Recovery ရဖို့ရာခိုင်နှုန်း နည်းပါတယ်။

Physical Extraction

Mobile Device ထဲကနေ လက်တလော ရှိနေတဲ့ Memory Storage အပြင် ဖုန်းထဲမှာရှိနေတဲ့ Internal Memory / External Memory တွေထဲကနေ အချက်အလက်အားလုံးကို Bit By Bit Copy ကူးယူတာဖြစ်ပါတယ်။(Recovery ပြန်လုပ်လိုတဲ့အတွက်ဖြစ်ပါတယ်) Mobile phone အမျိုးအစား အလိုက် Physical Extraction ရနိုင်မရနိုင်တာ တွေရှိပါသည်။ Physical Extraction အတွက် ဖုန်းကို Root ပြုလုပ်ရန်လိုအပ်ပါတယ်။ အချို့သော Security Path အားနည်းတဲ့ ဖုန်းတွေ Phone Recovery Partition မှာအားနည်းချက်ရှိတဲ့ ဖုန်းတွေသာ Physical ရယူနိုင်ပါတယ်။ များသောအားဖြင့် Model အနိမ့်ဖုန်းတွေများပါတယ်။

JTAG (Joint Test Action Group)

Mobile Phone ထုတ်လုပ်သူများက Mobile Ph အမျိုးအစားတစ်ခုကို တပ်ဆင် မထုတ်လုပ်ခင် တပ်ဆင်ထားတဲ့ Chip Set တွေ အမှား အယွင်းရှိ/မရှိ စစ်ဆေးပါတယ်။ အဲလိုစမ်းသပ်စစ်ဆေးဖို့အတွက် အချို့သောဖုန်း များမှာ JTAG Connector က ဖုန်းရဲ့ Circuit Board မှာပါရှိပါတယ်။ မပါရှိရင် Memory Chip ကို ရှာပြီး JTAG လုပ်ဖို့ အတွက် Wire ချိတ်ဆက်ဖို့ရှာပါမှာဖြစ်ပါတယ်။ TAP (Test Access Port) လုပ်တယ်လို့လဲ ခေါ်ပါတယ်။ချိတ်ဆက်လို့ရလျှင် Mobile Ph ရဲ့ Processor ကနေ Memory Chip ကို Command ပေးပြီး Full Memory Record ရအောင်ပြုလုပ်ပါတယ်။ Lock ဖြစ်နေတဲ့ ဖုန်းတွေတစ်စိတ်တစ်ပိုင်း ပျက်စီး နေတဲ့ဖုန်းတွေကို စစ်ဆေးဖို့ပြုလုပ်ရ ခြင်းဖြစ်ပါတယ်။

Chip OFF

JTAG အဆင့်နဲ့မရရင် ဖုန်းကနေ Memory Chip ကိုဖြုတ်ပြီး Chip Set Reader မှာတင်ပြီး Memory Chip ထဲက အချက်အလက်တွေကို ဖတ်တာဖြစ်ပါတယ်။ JATG လိုပဲ သီးသန့် ကျွမ်းကျင်သူတွေအပြင် အသုံးပြုရတဲ့ပစ္စည်းတွေလဲ လိုအပ်ပါတယ်။ ငွေကြေးကုန်ကျမှုပိုမိုများပြားပါတယ်။ Android 6.0 အထက်ဆိုရင် Encryption ကြောင့်အခက်အခဲရှိပါတယ်။

Micro Read

နောက်ဆုံးနည်းလမ်းဖြစ်ပါတယ်။ ကျွမ်းကျင်တဲ့ ပညာရှင်များ လိုအပ်ပါတယ်။ Memory Chip အပေါ်လွှာကို ဖယ်ရှားပြီး Chip ထဲက Gate တွေကို Microscope နဲ့ဖတ်တာဖြစ်ပါတယ်။ Gate တွေရဲ့ အနေအထားကိုကြည့်ပြီး Binary ကနေ Hex , HEX ကနေ Data သို့ပြောင်းလဲခြင်းဖြစ်ပါသည်။

IOS Device Acquisition

ဖုန်းကနေ ဖျက်ထားတဲ့ Call Log , Sms , Photo , Video ကို Recovery ပြန်ယူချင်လို့ Physical Acquisition လုပ်မယ်ဆိုရင်တော့ Apple Phone ကိုမေ့ထားရပါမယ်။ Mobile Forensics Products တွေကွဲပြားပေမဲ့ IOS Devices တွေကို Acquisition ရယူတဲ့နည်းလမ်းကတူညီတာတွေရှိပါတယ်။

Itunes Backup

ဖုန်းထဲကနေ Itunes Backup ဒါမှမဟုတ် Backup လုပ်ထားတဲ့ ကွန်ပျူတာထဲက ဒါမှမဟုတ် iCloud ထဲက Data ကိုရယူတာဖြစ်ပါတယ်။

Checkm8-Based Acquisition

Iphone 5 ကနေ Iphone X အထိရပါတယ်။Full File System နဲ့ Keychain ကိုရယူနိုင်ပါတယ်။ (No Need Jailbreak)

Agent Based Acquisition

Full File System နဲ့ Keychain ကိုရယူနိုင်ပါတယ်။ Iphone X ကနေ 12 Pro Max အထိ Support ပေးပါတယ်။ (No Need Jailbreak)

Media File Copy AFC Protocol

Photo Picture Video ကူးယူတာပါ။

Screen Capturing

Chat Log , Photo, Sms စတာတွေကို Forensics Products မှာပါတဲ့ Camera နဲ့ ဓာတ်ပုံရိုက်ယူတာပါ။

Android Phone Acquisition

ADB& ADB Pro Backup

Phone ထဲက Data ကို Internal Or External SD Card Or OTG ကနေ တစ်ဆင့် Backup ယူတာပါ။

Agent Base

Phone ထဲကို Forensics Products ရဲ့ Agent APK ထည့်ပြီး Data ကို ကူးယူတာပါ။ Backup လုပ်တဲ့သဘောတရားနဲ့ဆင်တူပါတယ်။

APK Downgrade

APK ကို မူရင်း Version ထက်နိမ့်တဲ့ APK ထည့်ပြီး APK ထဲကနေ Data ကို ရယူတာပါ။ ဒါ့အပြင် Qualcomm , MTK Chip အလိုက် Android Version, Security Patch အပေါ်မူတည်ပြီး ရယူတဲ့ နည်းလမ်းတွေရှိပါတယ်။

UFED4PC ဒါမှမဟုတ် UFED Touch ကနေ ဖုန်းအမျိုးအစားပေါ်မူတည်ပြီး သင့်တော်တဲ့ Extraction (Acquisition) နည်းလမ်းနဲ့ထုတ်ယူလိုက်တဲ့အခါမှာ အောက်ကပုံအတိုင်းရလာပါလိမ့်မယ်။

Name	Date modified	Type	Size
Samsung GSM_SM-G955FD Galaxy S8+	8/15/2020 9:35 PM	UFED Dump	64 KB
Samsung GSM_SM-G955FD Galaxy S8+.z01	8/15/2020 9:10 PM	Z01 File	1,048,576 KB
Samsung GSM_SM-G955FD Galaxy S8+.z02	8/15/2020 9:11 PM	Z02 File	1,048,576 KB
Samsung GSM_SM-G955FD Galaxy S8+.z03	8/15/2020 9:12 PM	Z03 File	1,048,576 KB
Samsung GSM_SM-G955FD Galaxy S8+.z04	8/15/2020 9:15 PM	Z04 File	1,048,576 KB
Samsung GSM_SM-G955FD Galaxy S8+.z05	8/31/2020 11:24 PM	Z05 File	1,048,576 KB
Samsung GSM_SM-G955FD Galaxy S8+.z06	8/31/2020 11:21 PM	Z06 File	1,048,576 KB
Samsung GSM_SM-G955FD Galaxy S8+.z07	8/31/2020 11:21 PM	Z07 File	1,048,576 KB
Samsung GSM_SM-G955FD Galaxy S8+	8/15/2020 9:34 PM	WinRAR ZIP archive	799,676 KB

ရလာတဲ့ File ကို UFED Physical Analyzer ထဲမှာထည့်ပြီး Analysis ပြုလုပ်တဲ့ အခါမှာ အောက်ကပုံအတိုင်းရလာလိမ့်မယ်။

UFED Physical Analyzer ထဲမှာထည့်ပြီး Analyszer လုပ်ပြီး ရလာတဲ့အဖြေကို Report သို့မဟုတ် UFED ကို Export လုပ်လို့ရပါတယ်။ ဒီနေရာမှာတော့ UFED READER အတွက် Export ထုတ်ပါတယ်။

Generate Report

General

Report Dataset
Samsung GSM_S...
Security
Formatting
Table Sorting
UFDR (For Celle...

General

File name: Samsung GSM_SM-G955FD Galaxy S8+ Rene Gade_2022-09-13_Report
Save to: C:\Users\aungz\Documents\My Reports Browse
Report sub directory: 2022-09-13.13-37-17
Project: Samsung GSM_SM-G955FD Galaxy S8+ Rene Gade
Format: UFDR (For Cellebrite Reader or Cellebrite Pathfinder)

Case Information
Examiner name:
Location:
Case number:
Case name:
Evidence number:
Department:
Organization:
Investigator:
Crime type:
Notes:

UFDR (For Cellebrite Reader or Cellebrite Pathfinder)
PDF Report
HTML Report
Excel Workbook (xlsx)
Word report
XML Report
Relativity Short Message Format
e-Discovery Load File
Close

UFED Reader အတွက် Export ထုတ်ရာမှာ Reader နဲ့ဖွင့်ကြည့်ရင် ပါစေချင်တဲ့ အပိုင်း မပါစေချင်တဲ့အပိုင်းကို သတ်မှတ်လို့ရပါတယ်။ ဒီနေရာမှာတော့ အကုန်နီးပါ Mark ပေးထားပါတယ်။ ရလာမဲ့ Extension File ကတော့ .UFDR ပဲဖြစ်ပါတယ်။ Hash အပိုင်းကတော့ အခုအချိန် ဥပဒေ၊ နည်းဥပဒေမရှိတဲ့အတွက် မထည့်ထားပါဘူး။ Tag ဆိုတာကတော့ Analysis လုပ်နေရင်း အရေးကြီးတဲ့ အချက်အလက်တွေ့ရင် တစ်ခါတည်း Analysis လုပ်ရင်းနဲ့ အရောင်နဲ့ခွဲခြား သတ်မှတ်တာ ဖြစ်ပါတယ်။

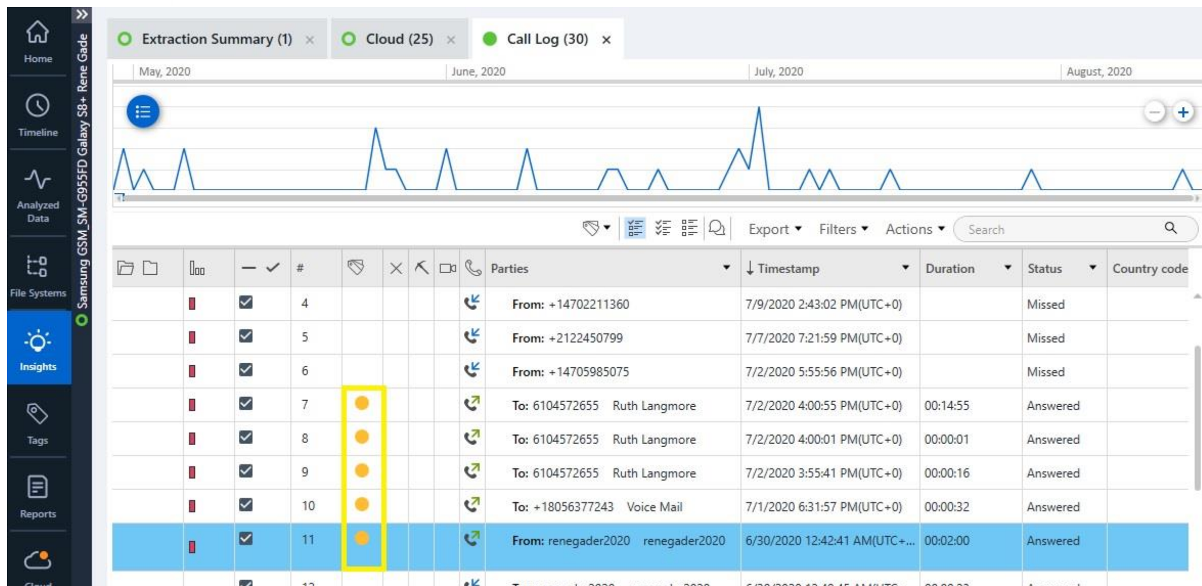
Report Dataset
Samsung GSM_...
Security
Formatting
Table Sorting
UFDR (For Celle...

Time range filter
Only events between these dates
From: Select a date
To: Select a date
Apply
Include items without a timestamp

Data types
Select/Deselect All
Enter text to filter ...

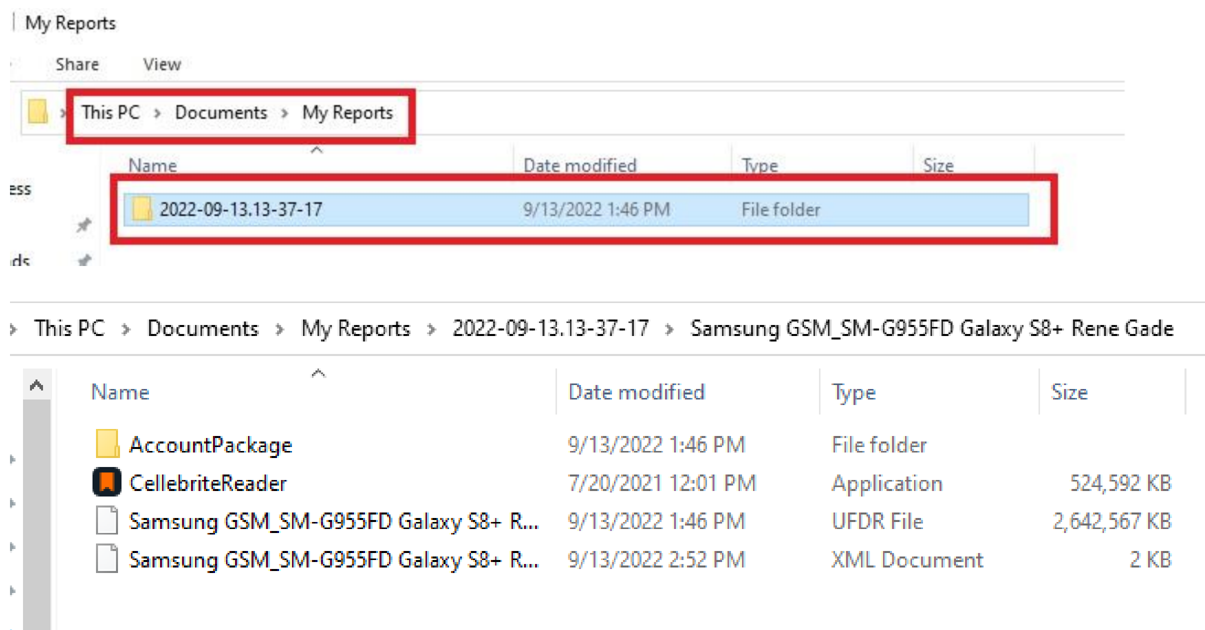
Applications (3/3)
Archives (147/147)
Audio (247/247)
Autofill (4/4)
Call Log (30/30)
Chats (64/64)
Configurations (50/50)
Contacts (65/65)
Cookies (688/688)
Databases (826/826)
Device Events (2/2)
Device Info (27/27)
Device Users (1/1)
Documents (6/6)
Downloads (1/1)
Emails (100/100)
Images (31303/31303)
Installed Applications (100/100)
Instant Messages (187/187)
Locations (66/66)
Passwords (355/355)
Searched Items (20/20)
Shortcuts (1/1)
Social Media (79/79)
Text (4372/4372)
Timeline (7698/7698)
Uncategorized (19910/19910)
User Accounts (30/30)
Videos (287/287)
Web History (1592/1592)
Wireless Networks (4062/4062)

Preferences
Tags table (0/0)
Tags only (0/0)
Select tags 0/0
Calculate SHA-2 (256 bit) hash
Include Hash set results
Redact all attachments
Include merged items (analyzed data)
Include merged items (data files)
Include Cellebrite Reader
Include source info indication

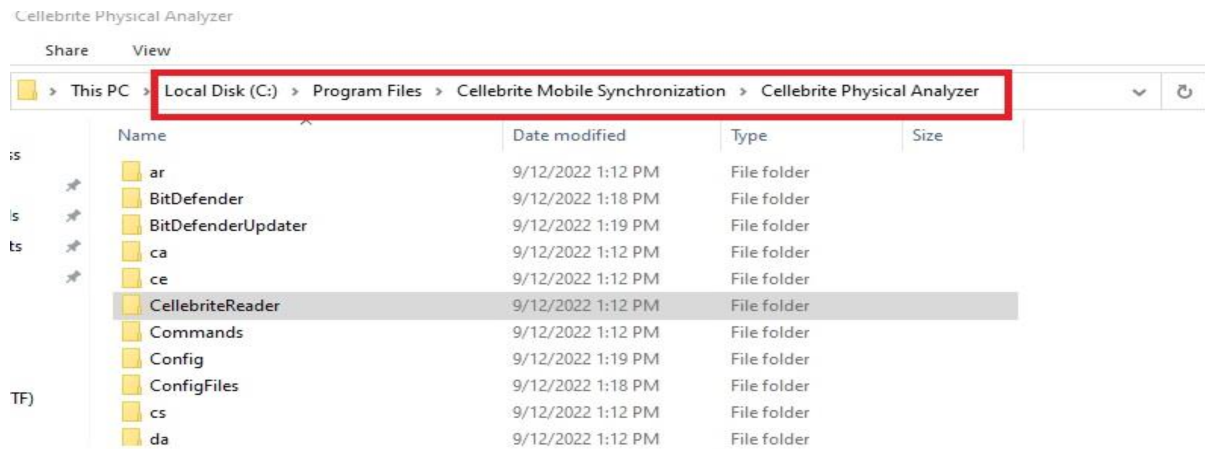


Physical Analyzer မှာ Analysis လုပ်နေရင်း အရေးကြီးတာတွေ့ရင် Tag လုပ်တာဖြစ်ပါတယ်။ Report OR UFED Reader မှာ Tag Only ပဲထည့်သွင်းနိုင်ပါတယ်။

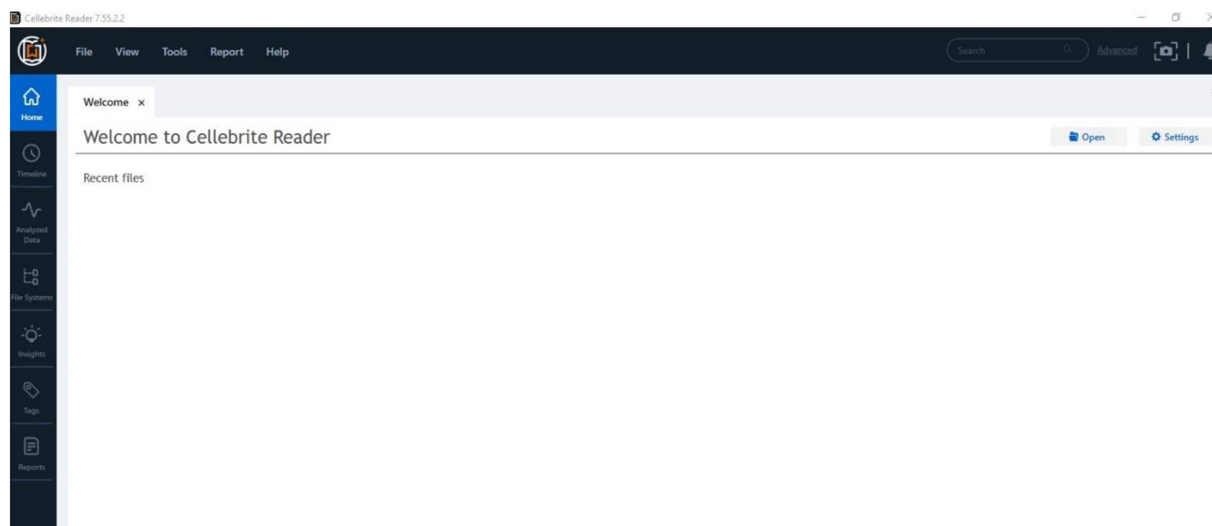
UFED Physical Analyzer ကနေ Reader အတွက် Report ထုတ်လိုက်တဲ့အခါမှာ Report ထုတ်တဲ့အချိန်နဲ့ Reader File ထွက်လာပါတယ်။

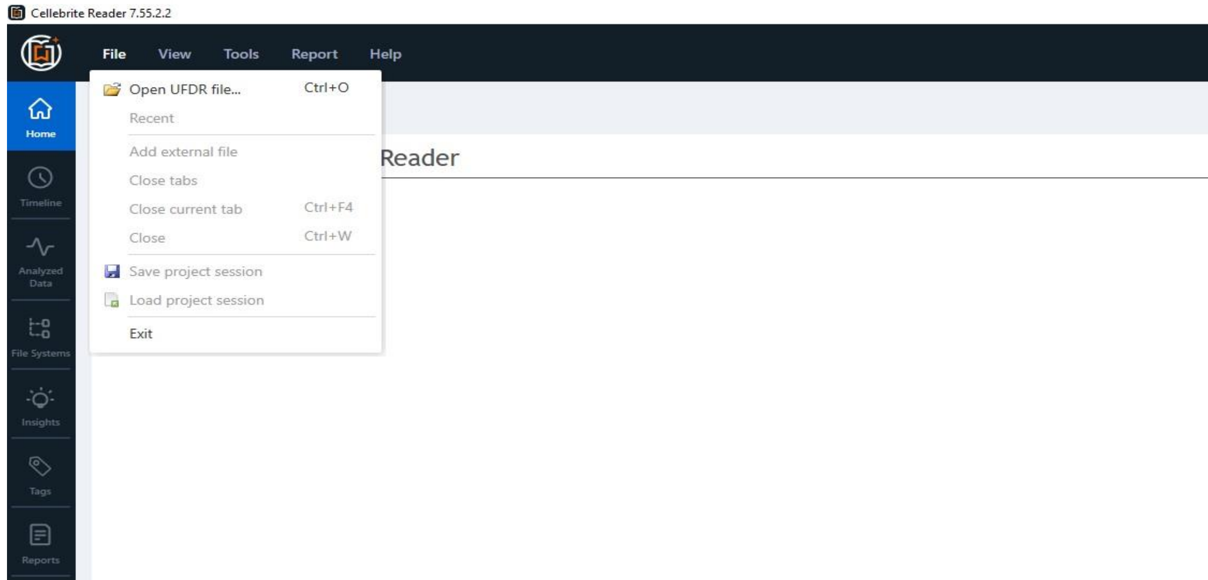


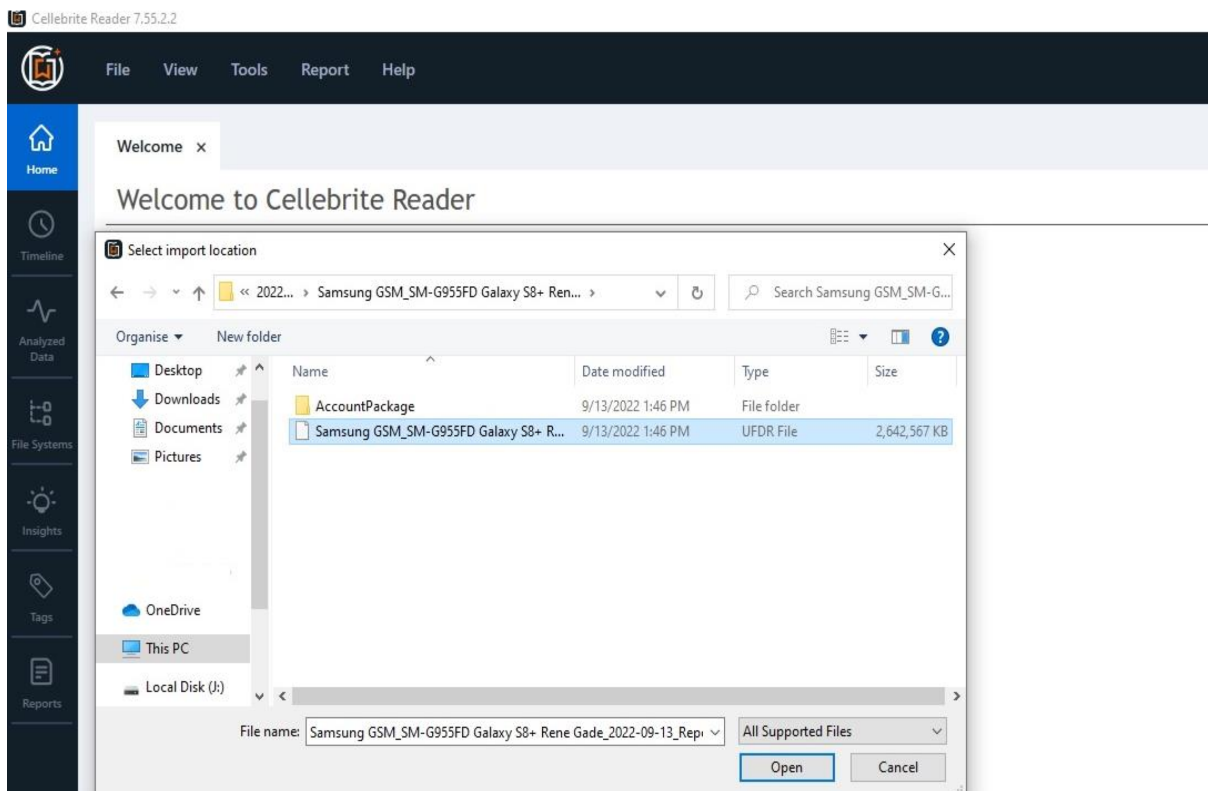
UFED Reader ကတော့ Analysis လုပ်တဲ့ UFED Physical Analyzer အတွင်းမှာ အသင့်ပါဝင်သလို Update File ကို Cellebrite Website မှာ အခမဲ့ Download ယူနိုင်ပါတယ်။ အခက်ခဲရှိရင် လိုင်စင်ပါတာကိုလာယူနိုင်ပါတယ်။ တင်ပေးထားရင် မကောင်းလို့ပါ။



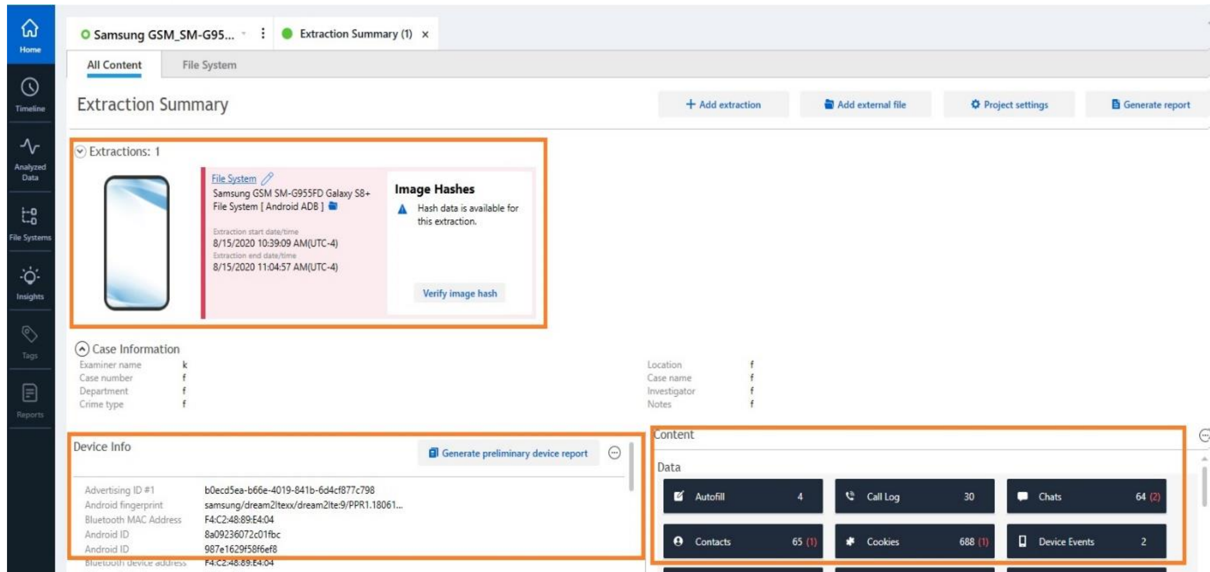
အောက်ကပုံကတော့ UFED Reader ပဲဖြစ်ပါတယ်။ Analysis အပိုင်းမှာပါတဲ့ Function တွေကလွဲရင် UFED Reader က UFED Physical Analyzer နဲ့ဆင်တူပါတယ်။





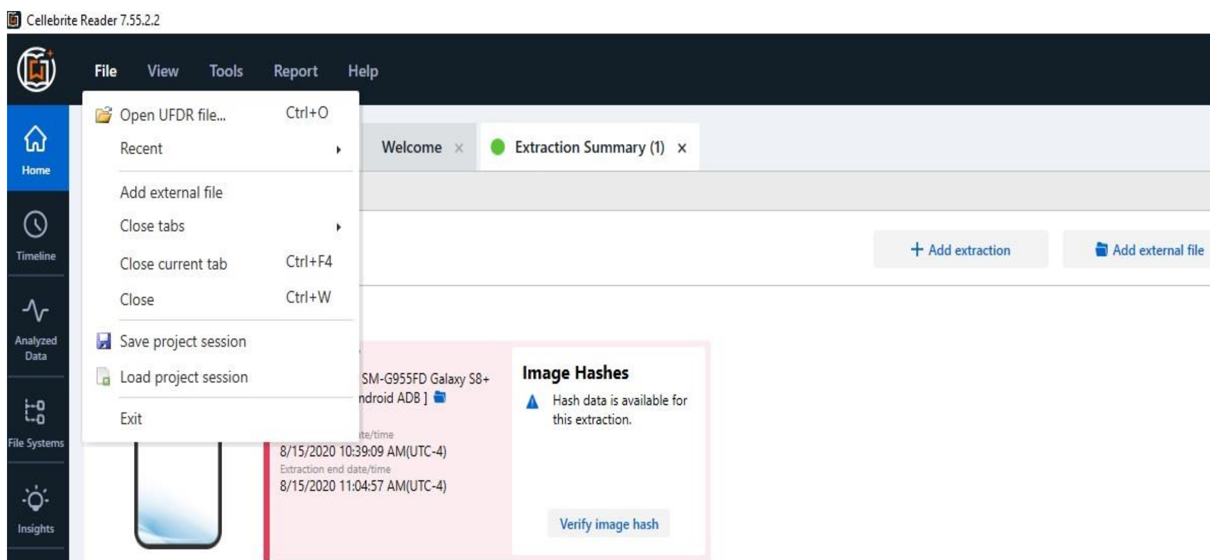


UFED Physical Analyzer ကနေရလာတဲ့ UFDR File ကို UFED READER ထဲ Import လုပ်တာဖြစ်ပါတယ်။ File Size အပေါ်မူတည်ပြီး ဖွင့်ဖို့အချိန်ကြာပါမယ်။

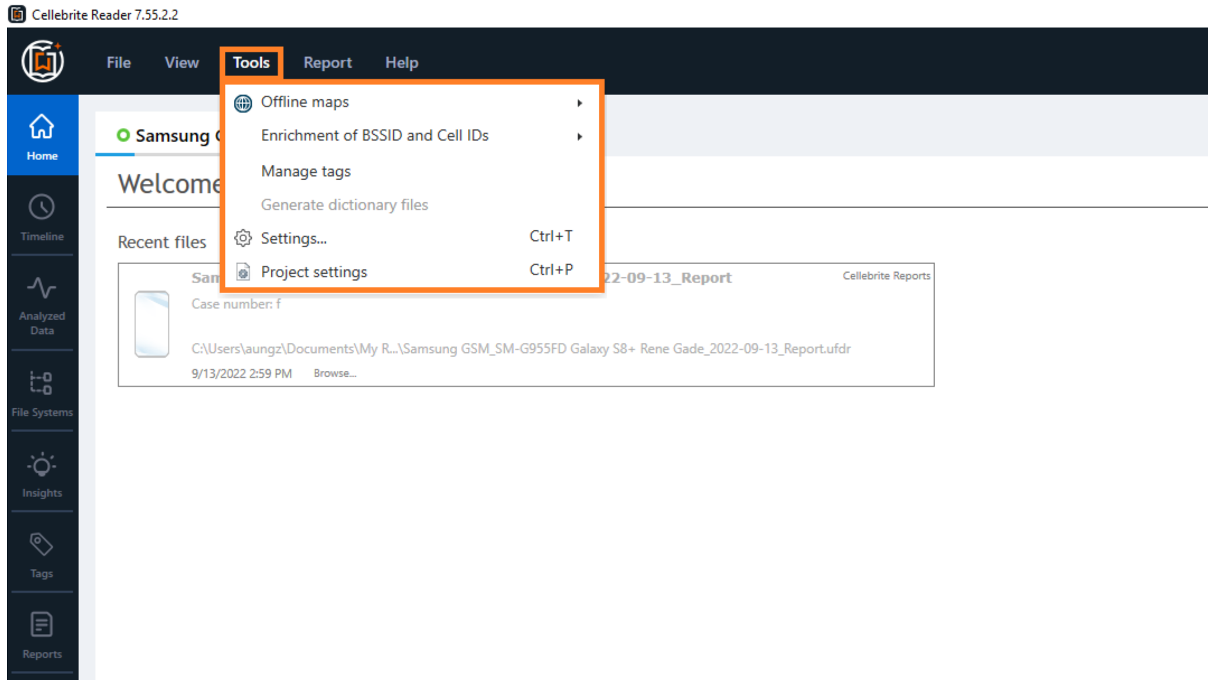


Import လုပ်လို့ပြီးတဲ့အခါမှာ UFED READER မှာမြင်ရမဲ့ ပုံဖြစ်ပါတယ်။ Extraction Date and time ကတော့ ဖုန်းကို စတင်စစ်ဆေးတဲ့အချိန်ဖြစ်ပါတယ်။ Extraction Method ကတော့ ဖုန်းကို File System Extraction ရယူထားကြောင်းကို ဖော်ပြထားပါတယ်။

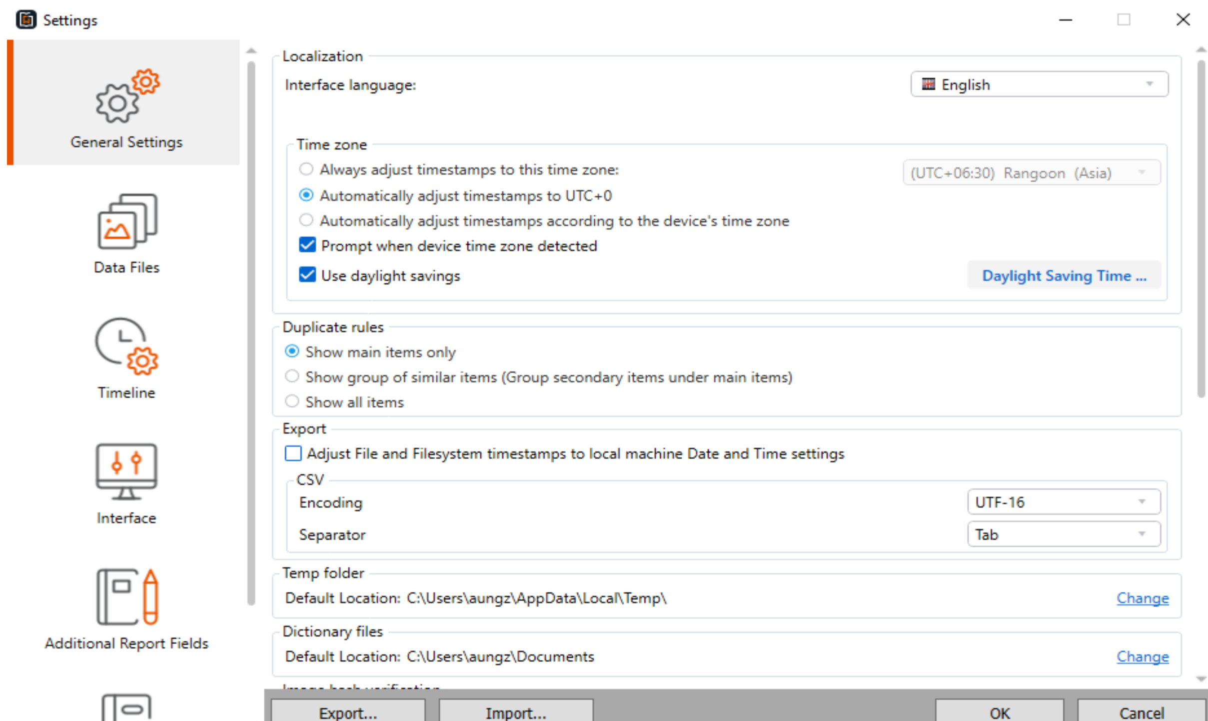
UFED READER မှာပါတဲ့ အရေးကြီးတဲ့ Menu အချို့ကိုဖော်ပြသွားပါမယ်။



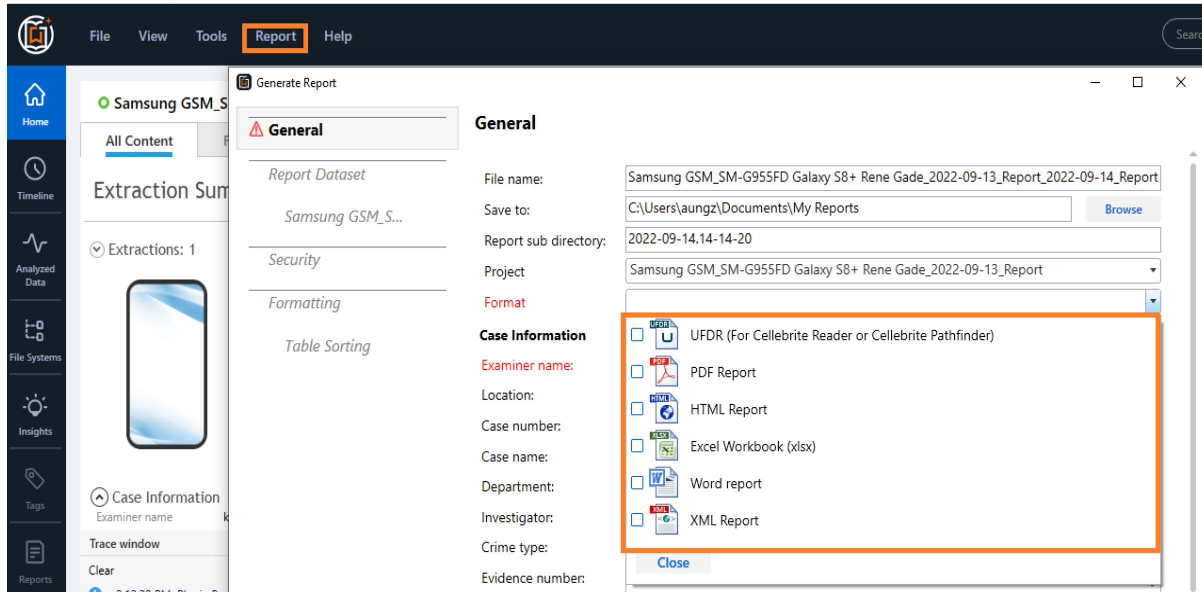
Add External ကတော့ ကျန်တဲ့ UFDR File ကိုပါထပ်ပြီးပေါင်းစပ်တာဖြစ်ပါတယ်။ ဥပမာ SIM CARD Data, USB Storage Data , Or Another Phone Or Tablet



Tools မှာတော့ Offline Map, Call Detail Record (CDR), WiFI အတွက် Map တွေ ထည့်သွင်းနိုင်ပါတယ်။ Tag ကတော့ ကိုယ့်အနေနဲ့ Reader မှာ Analysis လုပ်ရင် ထပ်တွေ့ရမဲ့ အရေးကြီးတာတွေ မှတ်ဖို့အတွက် အရောင်တွေ သတ်မှတ်နိုင်ပါတယ်။

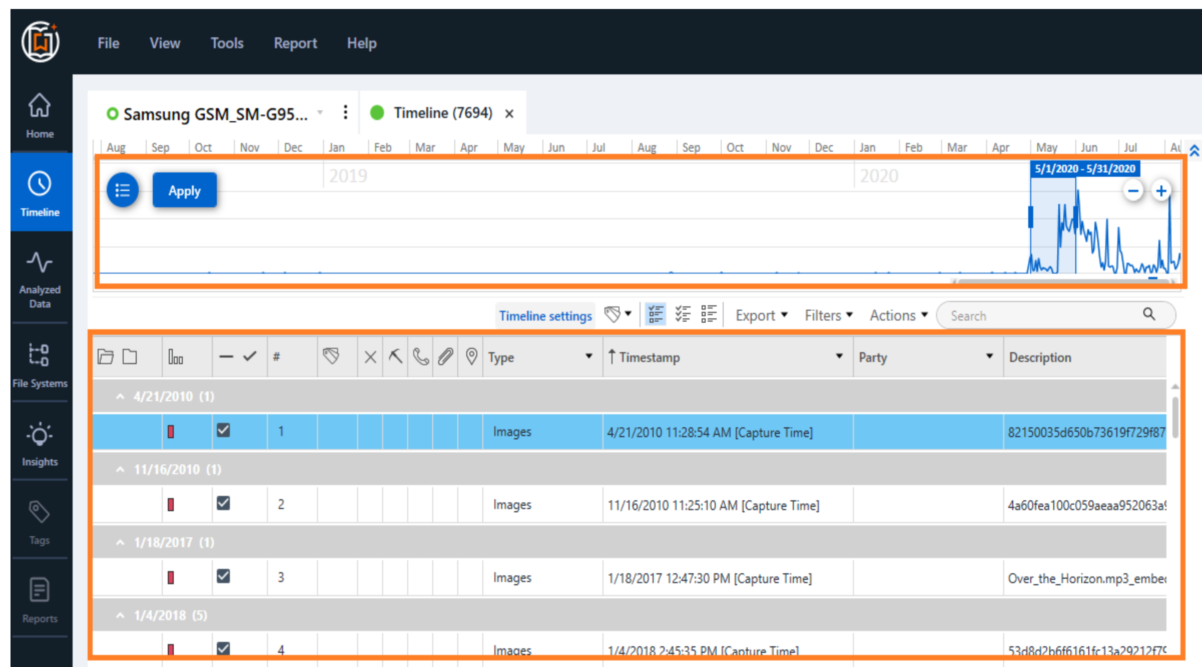


Settings ကတော့ ကိုယ်အသုံးပြုမဲ့ ပုံစံအပေါ်မူတည်ပြီး Reader မှာပြောင်းလဲ သတ်မှတ်နိုင်ပါတယ်။

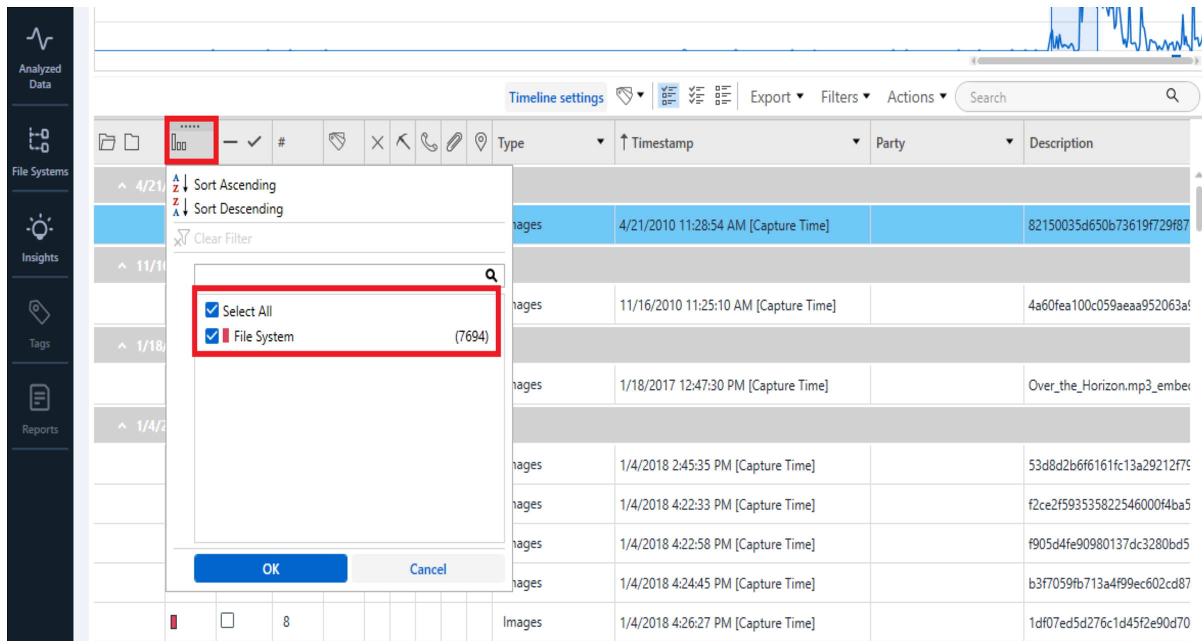


UFED Reader ကနေလဲ ထပ်ပြီး Report ပြုလုပ်နိုင်ပါတယ်။

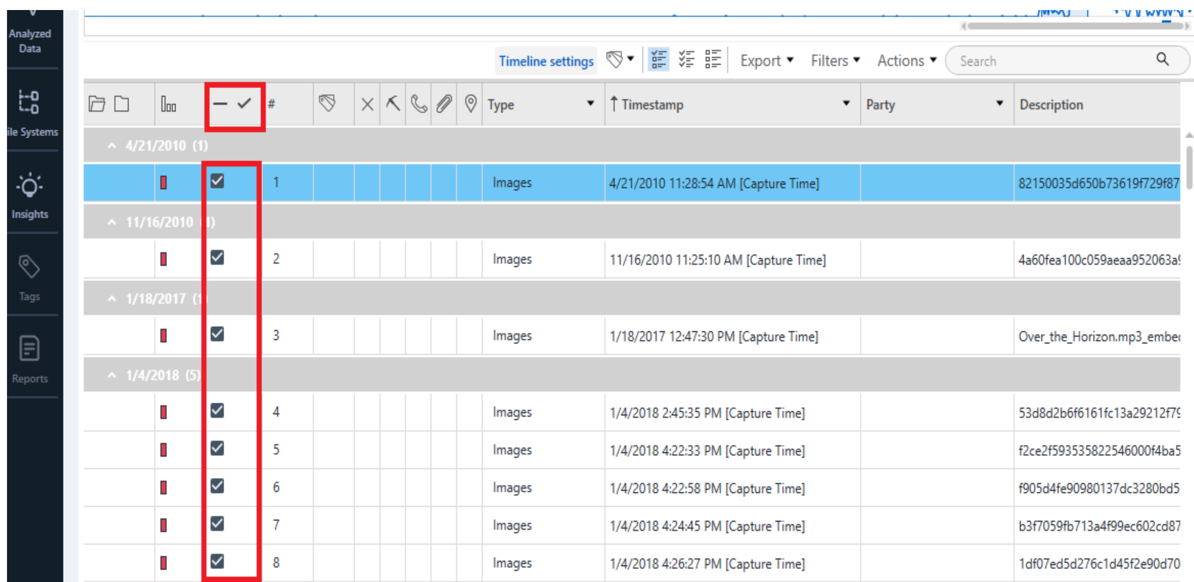
Time line



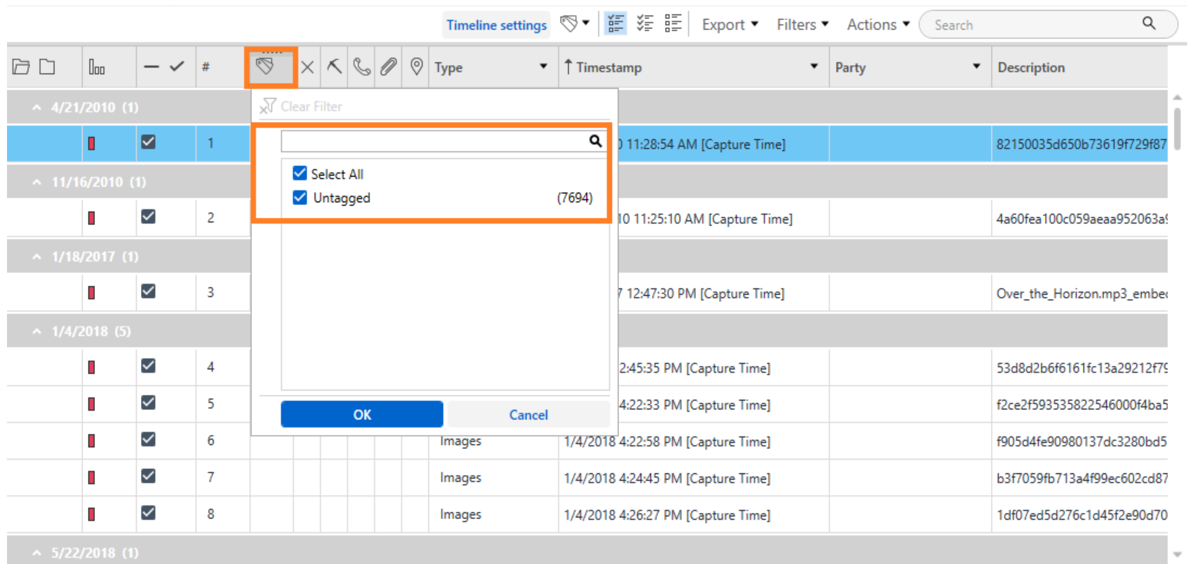
Time Line ကတော့ အချိန်ကာလအလိုက် ဘာတွေလုပ်ထားလဲဆိုတာကို ဖော်ပြတာဖြစ်ပါတယ်။ ကိုယ်ကြည့်ချင်တဲ့ ကာလအပိုင်းအခြားအပေါ်မူတည်ပြီး ရွေးချယ်သတ်မှတ်ပြီး ကြည့်နိုင်ပါတယ်။ နောက်ထပ်ဖော်ပြမှာကတော့ Time line မှာ အသုံးပြုလို့ရတဲ့ အကြောင်းအရာတွေ ဖြစ်ပါတယ်။



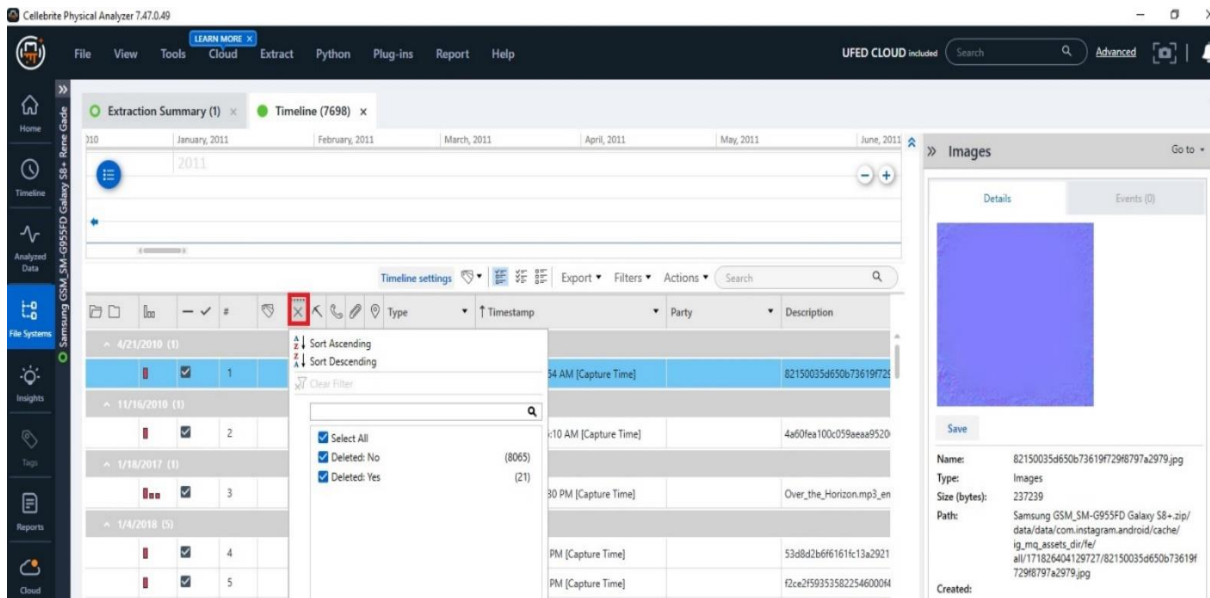
ဒါကတော့ File System Extraction ကနေရလာတဲ့အချက်အလက်တွေရလာတာ ကိုဖော်ပြထားတာဖြစ်ပါတယ်။



Report ထပ်ပြီးထုတ်ရင် အချက်အလက်တွေအကုန်ယူမှာလား မယူဘူးလား ဆိုတာ ကို ရွေးချယ်တာဖြစ်ပါတယ်။



Physical Analyzer မှာ Tag လုပ်ခဲ့တဲ့ အကြောင်းအရာတွေကို ပြသမှာ ဖြစ်ပါတယ်။အခုပုံမှာတော့ Tag လုပ်ထားခြင်းမရှိပါဘူး။

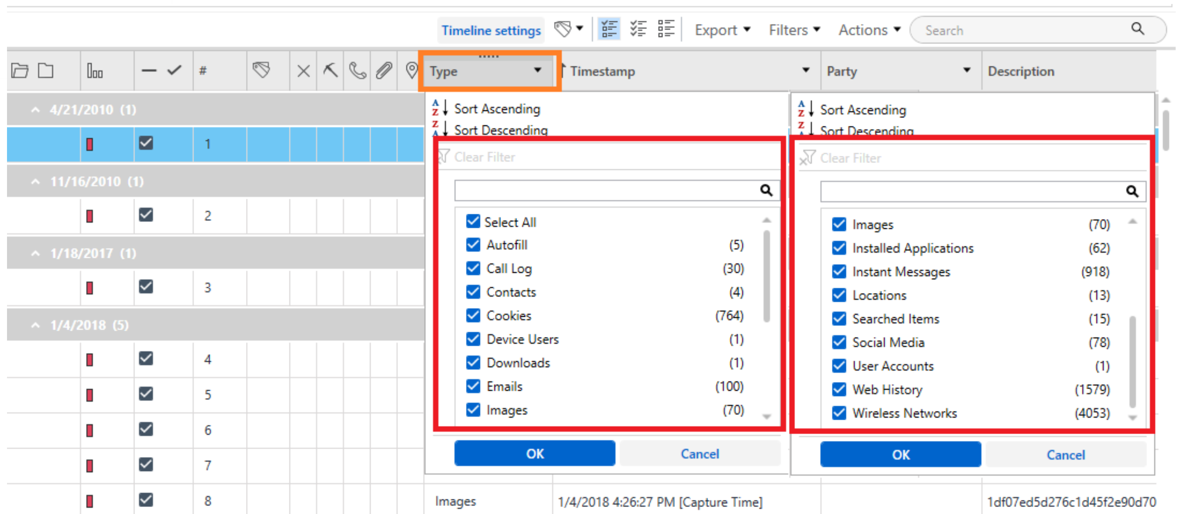


Delete လုပ်ထားတဲ့ File ဒါမှမဟုတ် Delete လုပ်မထားတဲ့ File တွေကို သီးသန့် Filter လုပ်ပြီးကြည့်နိုင်ပါတယ်။

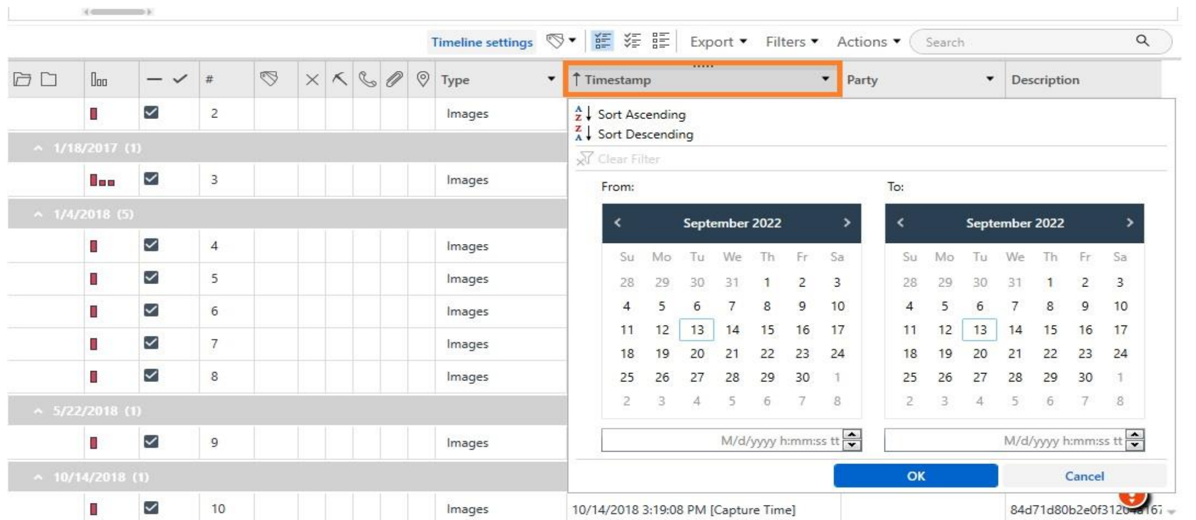
Unlocated Space ကနေရလာတဲ့ File တွေကို ဖော်ပြပေးပါတယ်။

Phone Call တွေကို သီးသန့် Filter လုပ်ပြီးကြည့်နိုင်ပါတယ်။

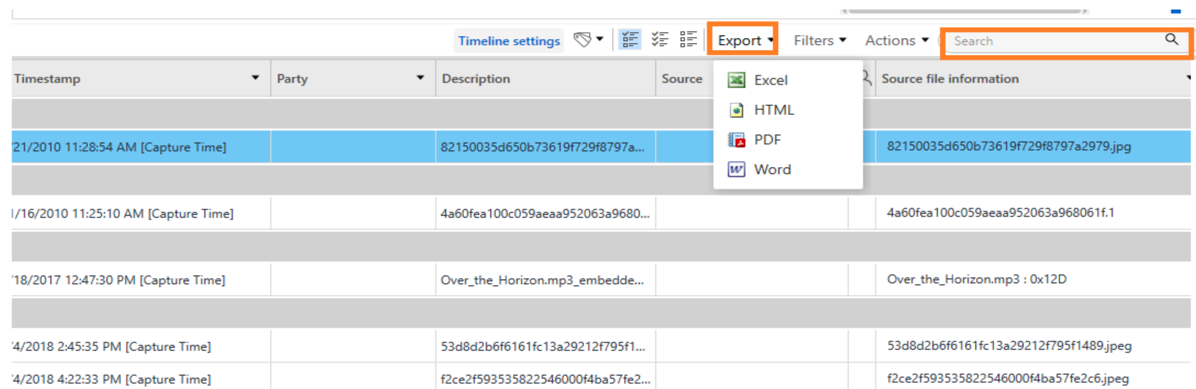
Location ပါတဲ့အကြောင်းအရာတွေကို Filter လုပ်ပြီးကြည့်နိုင်ပါတယ်။



ကိုယ် Analysis လုပ်ချင်တဲ့ အကြောင်းအရာပေါ်မူတည်ပြီး Filter လုပ်လို့ရပါတယ်။



အချိန်ကာလနဲ့ ထပ်ပြီး Filter လုပ်လို့ရပါတယ်။

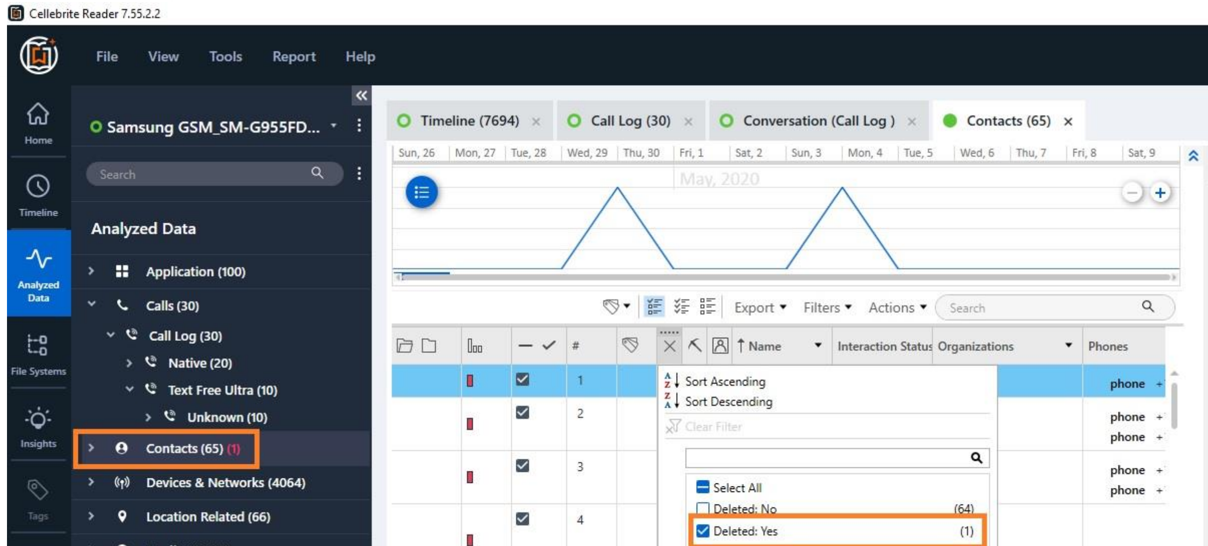


Report လုပ်တာတွေ အပြင် Case နဲ့ပတ်သတ်ပြီး ကိုယ်သက်ဆိုင်မယ် ထင်တဲ့ အကြောင်းအရာတွေကို ရှာဖွေနိုင်ပါတယ်။

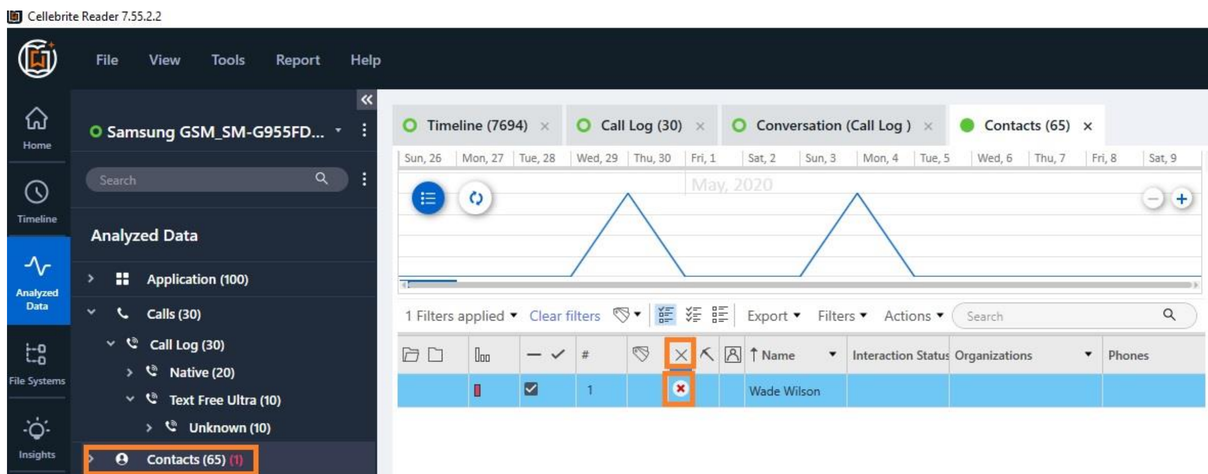
Analyzed Data

Analyzed Data မှာတော့ UFED Physical Analyzer ကနေ Analyzed လုပ်လို့ရလာတဲ့ Information တွေကို သက်ဆိုင်ရာ အပိုင်းလိုက်ခွဲပြီး ဖော်ပြထားပါတယ်။

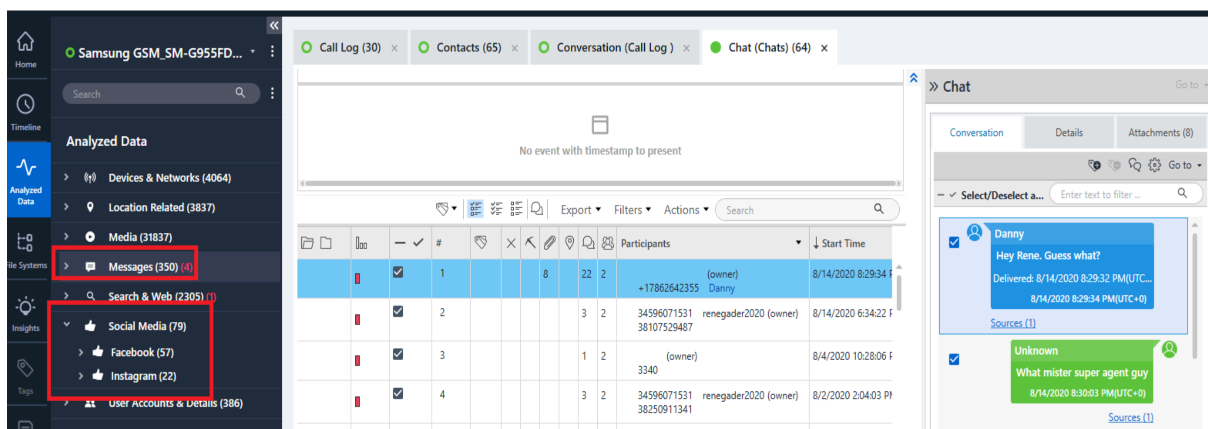
Call Log ကိုပဲ Filter အမျိုးမျိုး View အမျိုးမျိုး လုပ်ပြီး ကြည့်နိုင်ပါတယ်။



Contact ကိုမှ အနီရောင်နဲ့ပြထားတာက Recovery လုပ်ပြီးရလာတာ Contact တစ်ခုရှိ ကြောင်းပြတာဖြစ်ပါတယ်။

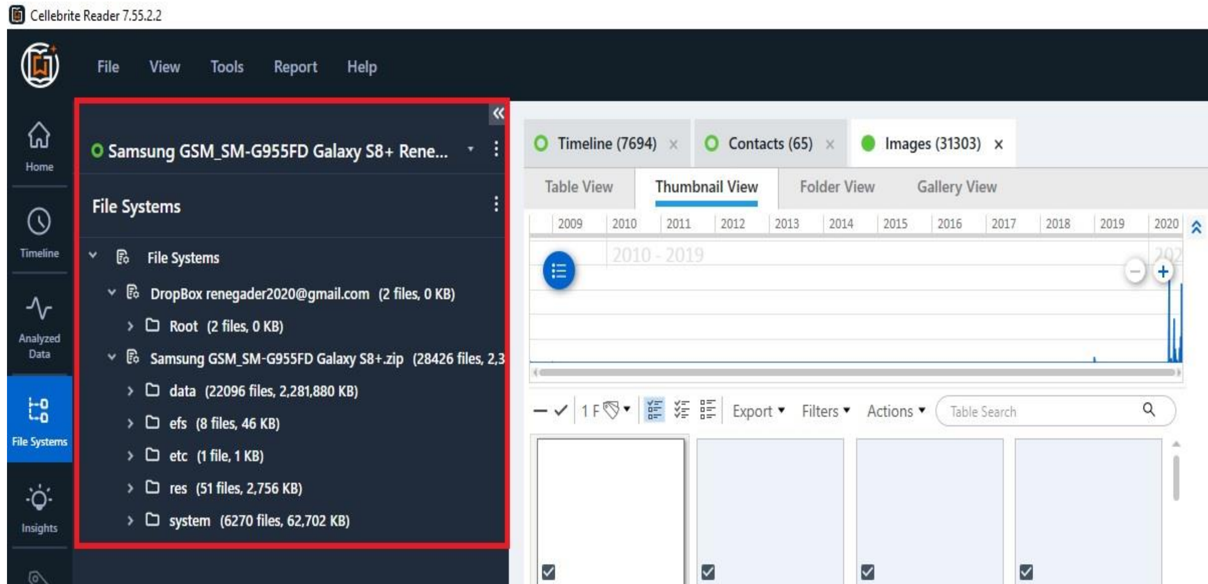


ဖျက်ထားတာ ဘယ်သူလဲဆိုတာကို Filter လုပ်ကြည့်တာဖြစ်ပါတယ်။



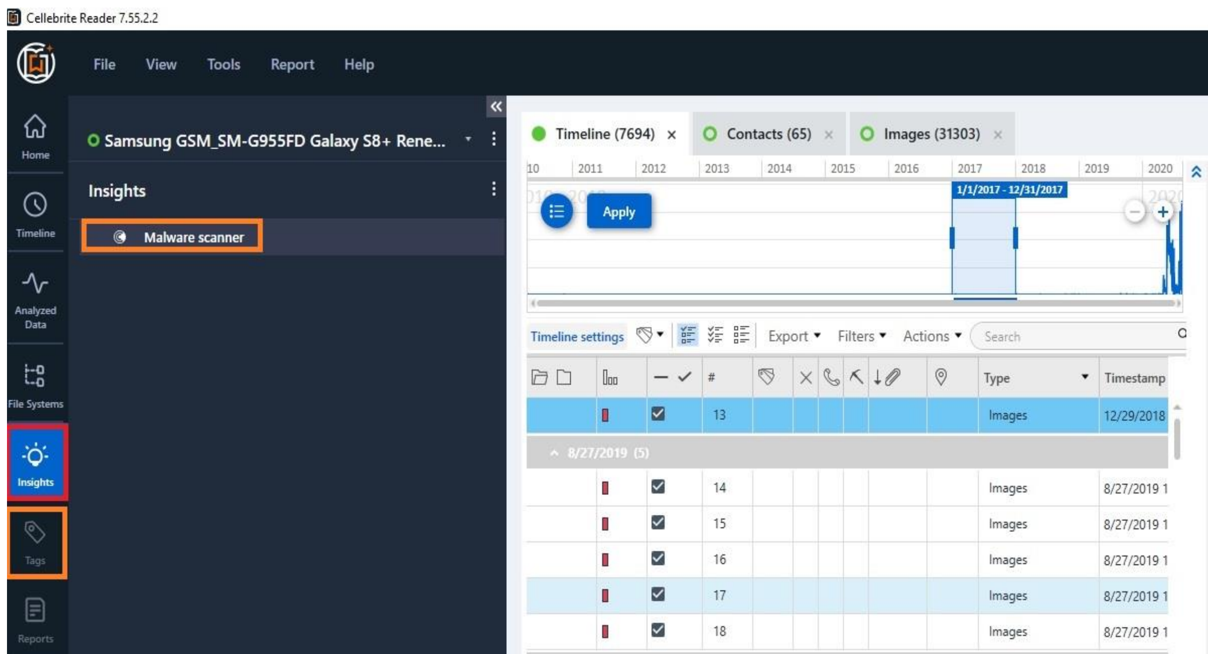
Message, Social Media & Web

File System



File System ကိုတော့ UFED Analyzer , UFED Reader တို့မှာ ဖော်ပြနိုင်ခြင်းမရှိတဲ့ အကြောင်းအရာတွေကို သီးသန့် Analysis လုပ်တဲ့နေရာမှာ အသုံးပြုတာဖြစ်ပါတယ်။

Insights



Insights ကတော့ Malware ပိုင်းအတွက် အသုံးပြုတာဖြစ်ပါတယ်။

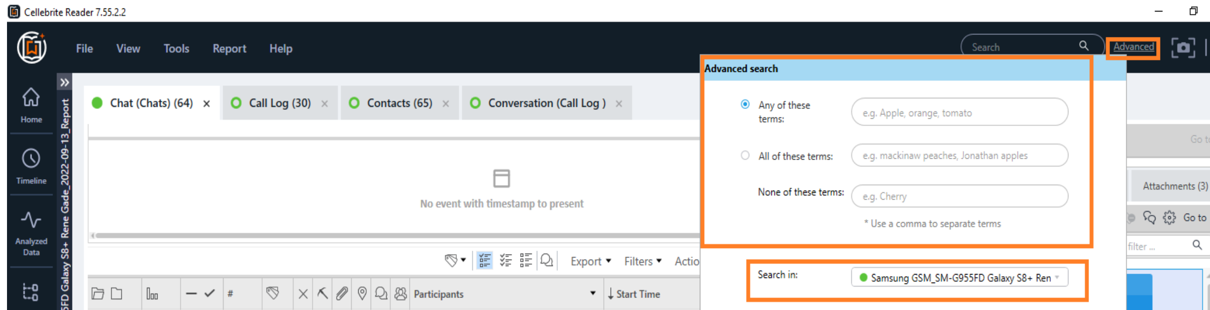
Tags & Reports

Tags ကတော့ UFED Reader မှာ ထပ်ပြီး အရေးပါတဲ့အကြောင်းအရာတွေကို ထပ်ပြီးမှတ်လိုက်ရင် Tags မှာ မှတ်ထားတာတွေကို ပြသပေးပါတယ်။

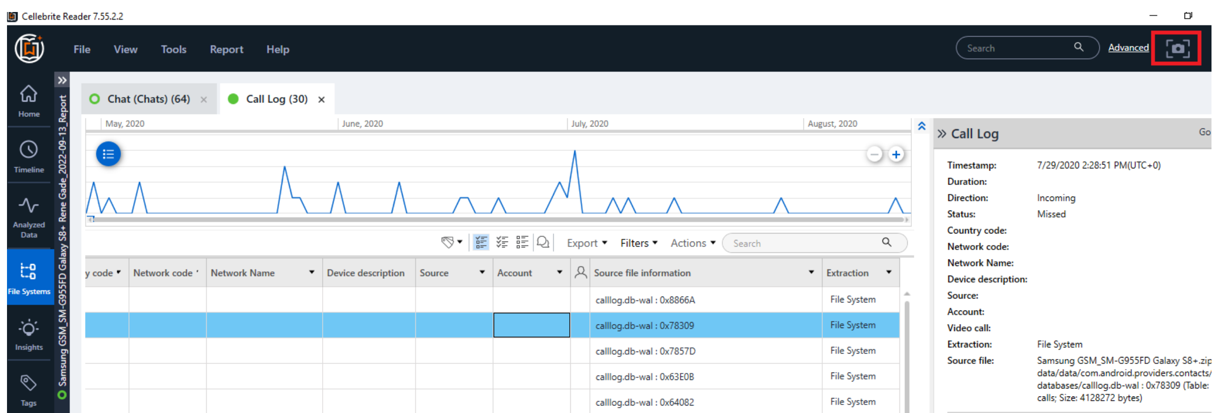
Report ကို Format အမျိုးမျိုးနဲ့ပြုလုပ်နိုင်ပါတယ်။

Advanced Search

Advanced Search မှာတော့ Case နဲ့ သက်ဆိုင်မဲ့ အကြောင်းအရာတွေကို ရှာဖွေနိုင်ပါတယ်။



Screen Shoot

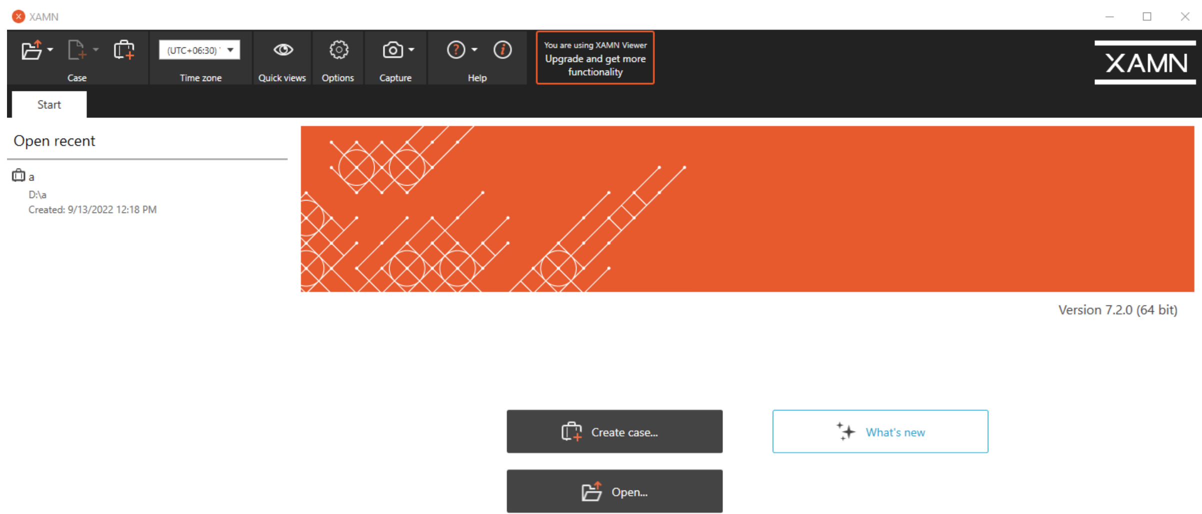


အခု UFED Reader နဲ့ပတ်သတ်ပြီး အကြမ်းဖျင်း ဖော်ပြပြီးပါပြီ။ ဆက်လက်ဖော်ပြမှာက World Wide မှာ အများဆုံးနောက်ထပ်သုံးတဲ့ MSAB (XRY) နဲ့ Oxygen Mobile Forensics အကြောင်းဖြစ်ပါတယ်။ UFED Reader ကိုအသုံးပြုတတ်ရင် ကျန်တာတွေကို လွယ်လွယ်ကူကူအသုံးပြုနိုင်ပါတယ်။ UFED READER အတွက် သိခြင်တာရှိရင် မေးနိုင်သလို လေ့လာချင်ရင် Reader နဲ့ UFED File ကို လာရောက်ယူနိုင်ပါတယ်။ အခြား Reader & Viewer တွေလဲအတူတူပါပဲ။ Case File တွေကိုလာယူနိုင်ပါတယ်။ သက်ဆိုင်ရာ Website တွေမှာလဲ Reader တွေကို အခမဲ့ Download ယူနိုင်ပါတယ်။ Reader တွေ Viewer တွေမှာ ပေါ်တဲ့ Analysis Data

တွေက စစ်ဆေးသူက Extraction (Acquisition) ပြုလုပ်တဲ့အနေအထားနဲ့ Reader ထဲကိုထည့်မထည့်ဆိုတဲ့ အပေါ်မူတည်ပါတယ်။

XAMN Viewer

XAMN Viewer ကတော့ Mobile Forensics Product ဖြစ်တဲ့ MSAB (XRY) ကနေ ရလာတဲ့ Case File ကို XAMN Viewer ထဲမှာထည့်ပြီးကြည့်နိုင်ပါတယ်။



Oxygen Forensics Viewer

Oxygen Forensics Viewer ကတော့ Mobile Forensics Product ဖြစ်တဲ့ Oxygen ကနေထွက်လာတဲ့ Case Backup File ကိုကြည့်နိုင်ပါတယ်။

